4. Immediate information processing consequences of QM

i.e., more examples of QM :)

√ (a) No-cloning theorem (NC 1.3.5, box 12.1)

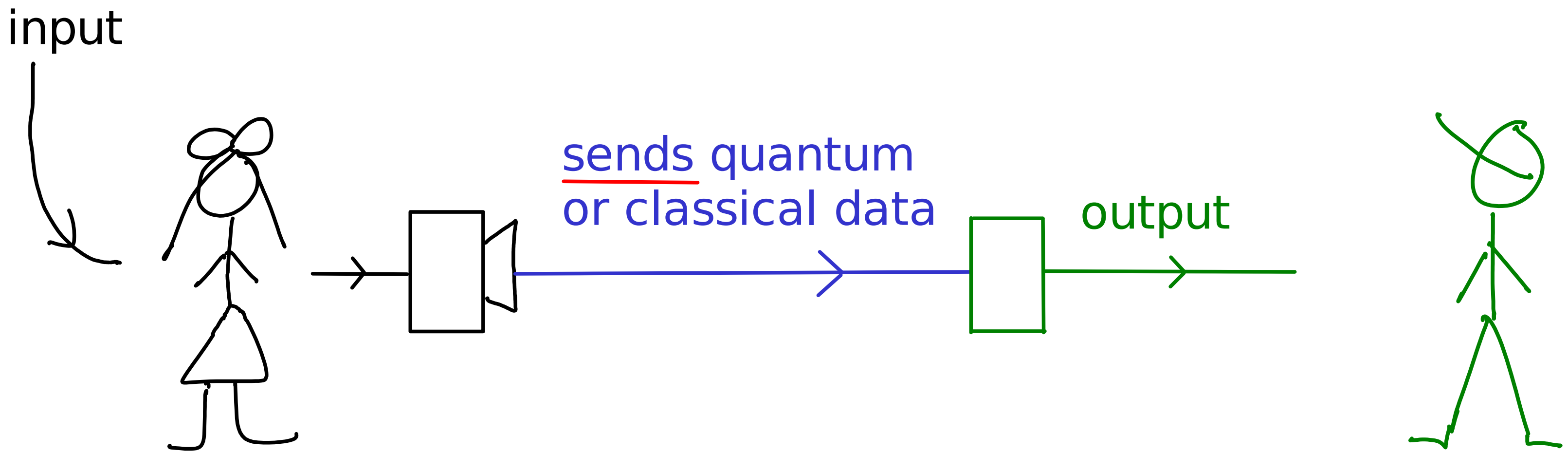
√ (b) Non-distinguishability of non-orthogonal states (NC p56-57)

√ (c) Communication of data
- protocols, bounds, and non-signalling principle
- encoding and extraction of classical data in QM

(d) Superdense coding and teleportation ←
√ (NC 2.3, 1.3.7, KLM 5.1-5.2, N 6.4-6.5)

(e) Bell's inequality and nonlocal games (NC 2.6, M 6.6)

Communication scenario from last time:



Alice (sender)

Bob (receiver)

If input data and output data are equal with high probability, or are similar, we say that the data is communicated from Alice to Bob.

What if Alice wants to communicate a quantum state to Bob by sending only classical data?

For simplicity, she wants to communicate a qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ to Bob.

What if Alice wants to communicate a quantum state to Bob by sending only classical data?

For simplicity, she wants to communicate a qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ to Bob.

Case (i): Alice knows a,b (she authors the message)

She can send approximations of a and b to Bob.
For Bob to decode a qubit closer and closer to $|\psi\rangle$ she has to send more and more bits.

What if Alice wants to communicate a quantum state to Bob by sending only classical data?

For simplicity, she wants to communicate a qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ to Bob.

Case (i): Alice knows a,b (she authors the message)

She can send approximations of a and b to Bob.
For Bob to decode a qubit closer and closer to $|\psi\rangle$ she has to send more and more bits.

Case (ii): Alice is given the state to be communicated
(she runs Qedex, usual setting)

What if Alice wants to communicate a quantum state to Bob by sending only classical data?

For simplicity, she wants to communicate a qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ to Bob.

Case (i): Alice knows a,b (she authors the message)

She can send approximations of a and b to Bob.
For Bob to decode a qubit closer and closer to $|\psi\rangle$ she has to send more and more bits.

Case (ii): Alice is given the state to be communicated (she runs Qedex, usual setting)

She does not know a,b, and cannot know more than 1 bit of information about them by Holevo's bound.

Can't comm quantum states by sending classical data.

Free entanglement is like free love

-- it changes the world.

Charles Bennett, Cambridge, 1999

Teleportation

Alice can communicate a qubit to Bob
if (1) she can send 2 classical bits to Bob, and
(2) they share the ebit $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

How to think about quantum protocols:

Which party has what classical/quantum information ?

Which party has what quantum system ?

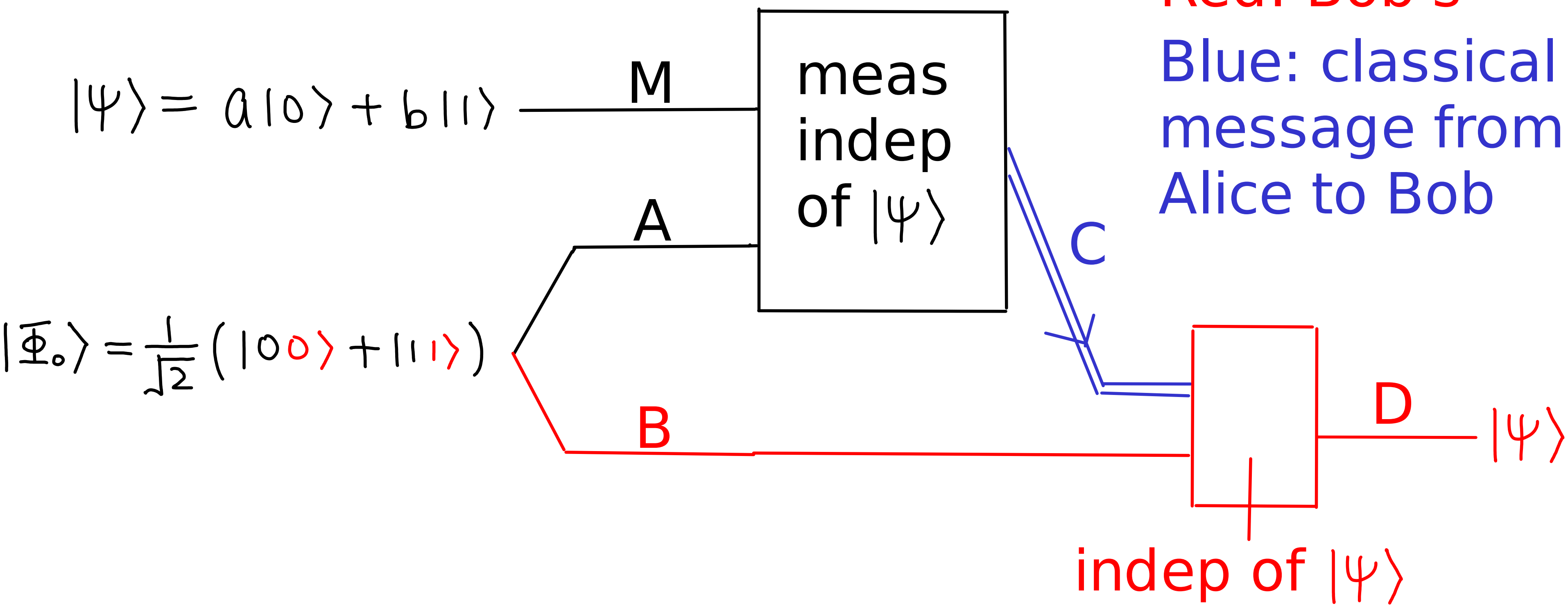
What operations he/she is allowed to do ?

Teleportation

Alice can communicate a qubit to Bob
if (1) she can send 2 classical bits to Bob, and
(2) they share the ebit $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Schematic diagram to be completed:

Black: Alice's
Red: Bob's
Blue: classical message from Alice to Bob



Main mathematical tool:
Expressing an 8-dim quantum state in 2 ways.

$$(a|0\rangle + b|1\rangle)_M \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$$

$$= (a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)_{MAB} \frac{1}{\sqrt{2}}$$

Main mathematical tool:
Expressing an 8-dim quantum state in 2 ways.

$$(a|0\rangle + b|1\rangle)_M \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$$

$$= (a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)_{MAB} \frac{1}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}(a|0\rangle + b|1\rangle)_B \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}(a|0\rangle - b|1\rangle)_B \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}(a|1\rangle + b|0\rangle)_B \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}(a|1\rangle - b|0\rangle)_B \frac{1}{2}$$

Main mathematical tool:
Expressing an 8-dim quantum state in 2 ways.

$$(a|0\rangle + b|1\rangle)_M \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$$

$$= (a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)_{MAB} \frac{1}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}(a|0\rangle + b|1\rangle)_B \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}(a|0\rangle - b|1\rangle)_B \frac{1}{2}$$

no cross terms gives $a|000\rangle + b|111\rangle$

$$+ \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}(a|1\rangle + b|0\rangle)_B \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}(a|1\rangle - b|0\rangle)_B \frac{1}{2}$$

Main mathematical tool:
Expressing an 8-dim quantum state in 2 ways.

$$(a|0\rangle + b|1\rangle)_M \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$$

$$= (a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)_{MAB} \frac{1}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}(a|0\rangle + b|1\rangle)_B \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}(a|0\rangle - b|1\rangle)_B \frac{1}{2}$$

no cross terms gives $a|000\rangle + b|111\rangle$

$$+ \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}(a|1\rangle + b|0\rangle)_B \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}(a|1\rangle - b|0\rangle)_B \frac{1}{2}$$

$= a|011\rangle + b|100\rangle$

$$\underbrace{(a|0\rangle + b|1\rangle)_M}_{|\psi\rangle} \underbrace{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}}_{|\Phi_0\rangle} =$$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}(a|0\rangle + b|1\rangle)_B \ \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}(a|0\rangle - b|1\rangle)_B \ \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}(a|1\rangle + b|0\rangle)_B \ \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}(a|1\rangle - b|0\rangle)_B \ \frac{1}{2}$$

Pauli's: $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Bell basis: $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\Phi_y\rangle = \frac{1}{\sqrt{2}}(i|10\rangle - i|01\rangle)$

$|\Phi_x\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$, $|\Phi_z\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

$|\psi\rangle$ → $(a|0\rangle + b|1\rangle)_M$, $|\Phi_0\rangle$ → $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$

$$(a|0\rangle + b|1\rangle)_M \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} =$$

$|\Phi_0\rangle$ → $$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}(a|0\rangle + b|1\rangle)_B \ \frac{1}{2}$$

$|\Phi_z\rangle$ → $$+\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}(a|0\rangle - b|1\rangle)_B \ \frac{1}{2}$$

$|\Phi_x\rangle$ → $$+\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}(a|1\rangle + b|0\rangle)_B \ \frac{1}{2}$$

$i|\Phi_y\rangle$ → $$+\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}(a|1\rangle - b|0\rangle)_B \ \frac{1}{2}$$

Pauli's: $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Bell basis:

$$|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi_y\rangle = \frac{1}{\sqrt{2}}(i|10\rangle - i|01\rangle)$$

$$|\Phi_x\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle), \quad |\Phi_z\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$|\psi\rangle$, $|\Phi_0\rangle$

$$\overbrace{(a|0\rangle + b|1\rangle)_M}^{|\psi\rangle} \overbrace{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}}^{|\Phi_0\rangle} =$$

$$|\Phi_0\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}\,(a|0\rangle + b|1\rangle)_B\ \frac{1}{2} \leftarrow |\psi\rangle$$

$$|\Phi_z\rangle \rightarrow + \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}\,(a|0\rangle - b|1\rangle)_B\ \frac{1}{2} \leftarrow \sigma_z|\psi\rangle$$

$$|\Phi_x\rangle \rightarrow + \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}\,(a|1\rangle + b|0\rangle)_B\ \frac{1}{2} \leftarrow \sigma_x|\psi\rangle$$

$$i|\Phi_y\rangle \rightarrow + \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}\,(a|1\rangle - b|0\rangle)_B\ \frac{1}{2} \leftarrow \sigma_y|\psi\rangle / i$$

Pauli's: $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Bell basis:

$$|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi_y\rangle = \frac{1}{\sqrt{2}}(i|10\rangle - i|01\rangle)$$

$$|\Phi_x\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle), \quad |\Phi_z\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$\underbrace{(a|0\rangle + b|1\rangle)_M}_{|\psi\rangle} \, \underbrace{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}}_{|\Phi_0\rangle} =$$

$$\underbrace{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}}_{|\Phi_0\rangle} \underbrace{(a|0\rangle + b|1\rangle)_B}_{|\psi\rangle} \frac{1}{2}$$

$$+ \underbrace{\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}}_{|\Phi_z\rangle} \underbrace{(a|0\rangle - b|1\rangle)_B}_{\sigma_z|\psi\rangle} \frac{1}{2}$$

$$+ \underbrace{\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}}_{|\Phi_x\rangle} \underbrace{(a|1\rangle + b|0\rangle)_B}_{\sigma_x|\psi\rangle} \frac{1}{2}$$

$$+ \underbrace{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}}_{i|\Phi_y\rangle} \underbrace{(a|1\rangle - b|0\rangle)_B}_{\sigma_y|\psi\rangle / i} \frac{1}{2}$$

If Alice measures MA along the Bell basis, each outcome $k \in \{0,x,y,z\}$ occurs with prob 1/4, and postmeasurement state is $|\Phi_k\rangle_{MA} \otimes \sigma_k |\psi\rangle_B$.

$$
\underbrace{(a|0\rangle + b|1\rangle)_M}_{|\psi\rangle} \underbrace{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}}_{|\Phi_0\rangle} =
$$

$$
\begin{aligned}
&\underbrace{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}}_{|\Phi_0\rangle} \underbrace{(a|0\rangle + b|1\rangle)_B}_{|\psi\rangle} \ \frac{1}{2} \\
+ &\underbrace{\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}}_{|\Phi_z\rangle} \underbrace{(a|0\rangle - b|1\rangle)_B}_{\sigma_z|\psi\rangle} \ \frac{1}{2} \\
+ &\underbrace{\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}}_{|\Phi_x\rangle} \underbrace{(a|1\rangle + b|0\rangle)_B}_{\sigma_x|\psi\rangle} \ \frac{1}{2} \\
+ &\underbrace{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}}_{i|\Phi_y\rangle} \underbrace{(a|1\rangle - b|0\rangle)_B}_{\sigma_y|\psi\rangle / i} \ \frac{1}{2}
\end{aligned}
$$

If Alice measures MA along the Bell basis, each outcome $k \in \{0,x,y,z\}$ occurs with prob 1/4, and postmeasurement state is $|\Phi_k\rangle_{MA} \otimes \sigma_k |\psi\rangle_B$.

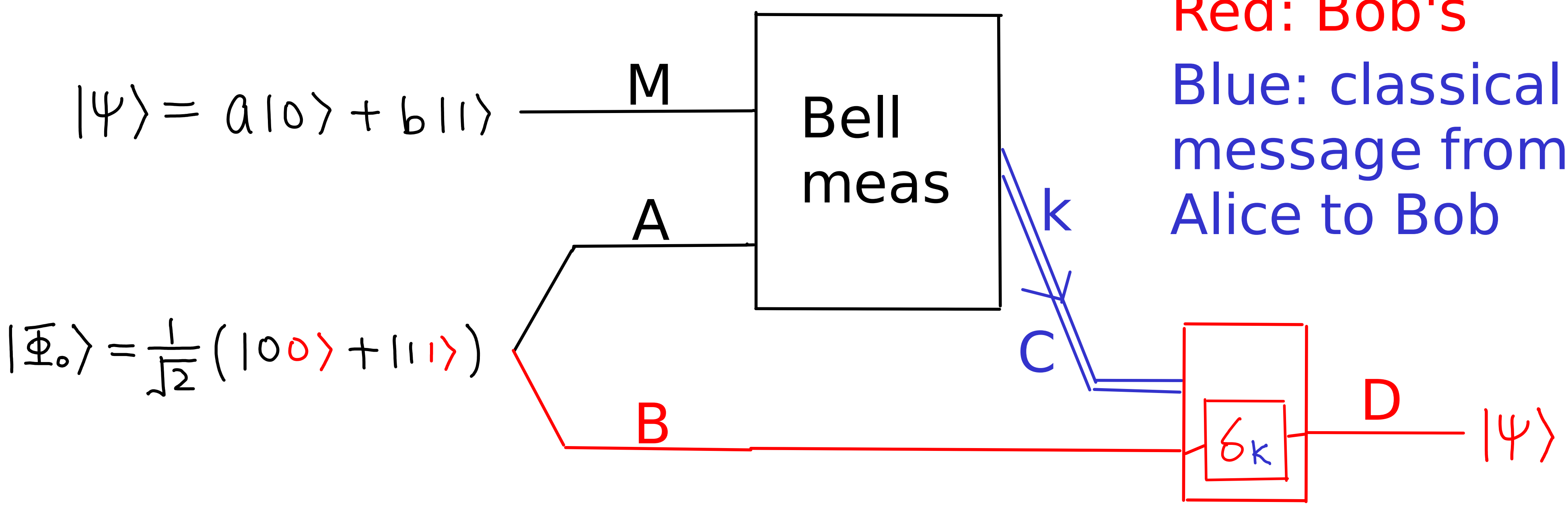
If Alice sends k to Bob, he can apply σ_k to B, turning $\sigma_k |\psi\rangle_B$ to $|\psi\rangle_B$.

Teleportation

Alice can communicate a qubit to Bob
if (1) she can send 2 classical bits to Bob, and
  (2) they share the ebit $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Schematic diagram:

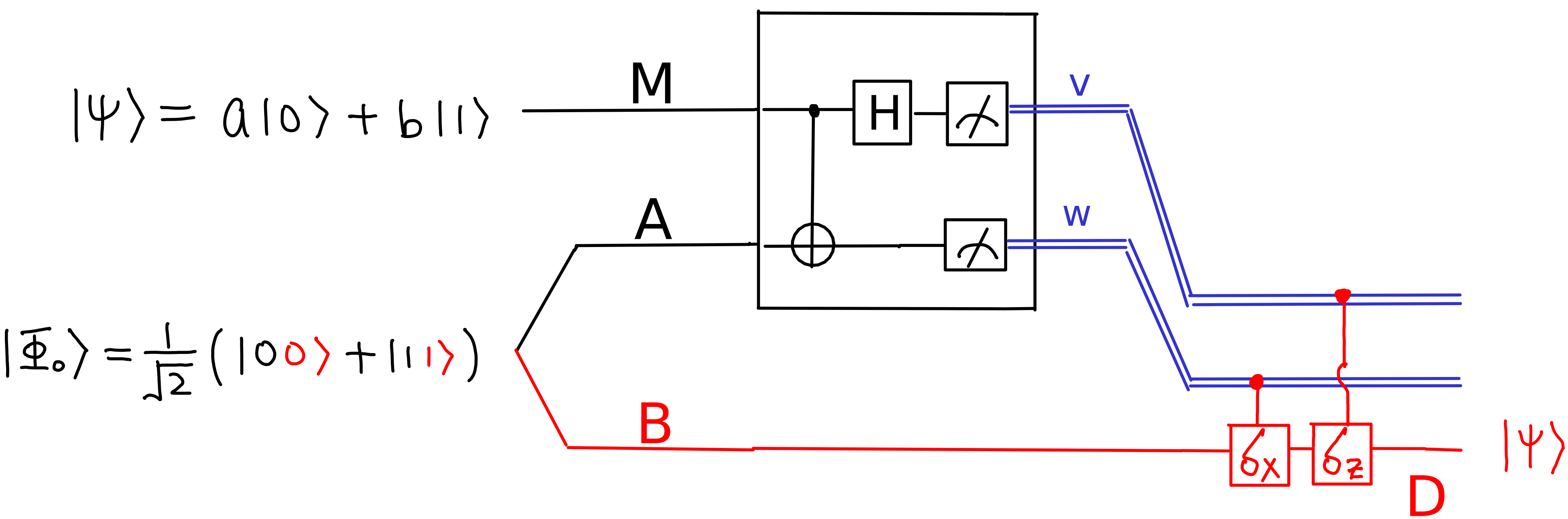
Black: Alice's
Red: Bob's
Blue: classical message from Alice to Bob



Teleportation

Alice can communicate a qubit to Bob
if (1) she can send 2 classical bits to Bob, and
(2) they share the ebit $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Exercise: verify the following specific implementation



Here, k is given by 2 bits (v,w). Note also $\sigma_y = i\,\sigma_z \cdot \sigma_x$.

PHYSICAL REVIEW
LETTERS

VOLUME 70 29 MARCH 1993 NUMBER 13

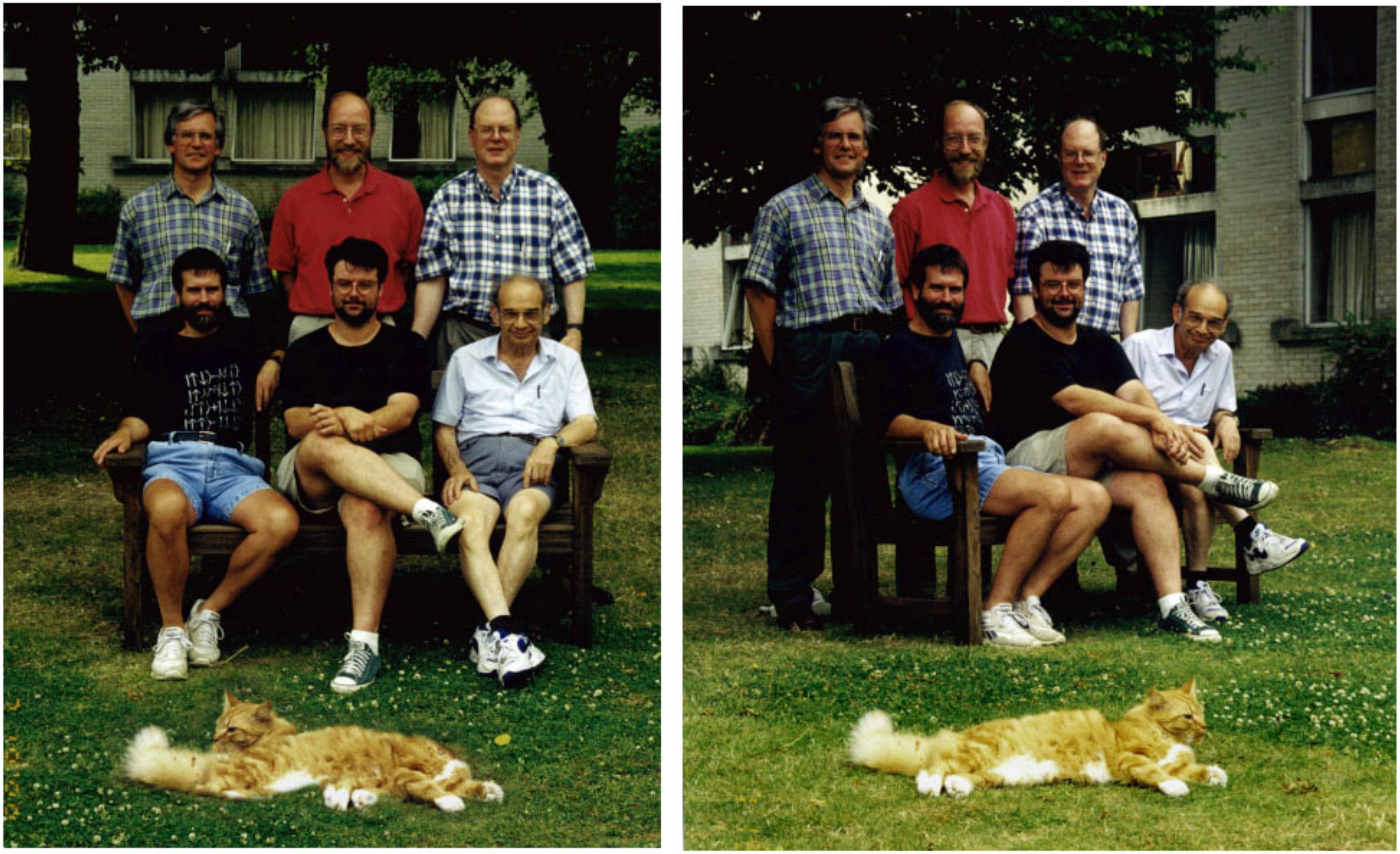
Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels

Charles H. Bennett,[1] Gilles Brassard,[2] Claude Crépeau,[2],[3]
Richard Jozsa,[2] Asher Peres,[4] and William K. Wootters[5]
[1] *IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York 10598*
[2] *Département IRO, Université de Montréal, C.P. 6128, Succursale "A", Montréal, Québec, Canada H3C 3J7*
[3] *Laboratoire d'Informatique de l'École Normale Supérieure, 45 rue d'Ulm, 75230 Paris CEDEX 05, France*[a]
[4] *Department of Physics, Technion–Israel Institute of Technology, 32000 Haifa, Israel*
[5] *Department of Physics, Williams College, Williamstown, Massachusetts 01267*
(Received 2 December 1992)

An unknown quantum state $|\phi\rangle$ can be disassembled into, then later reconstructed from, purely classical information and purely nonclassical Einstein-Podolsky-Rosen (EPR) correlations. To do so the sender, "Alice," and the receiver, "Bob," must prearrange the sharing of an EPR-correlated pair of particles. Alice makes a joint measurement on her EPR particle and the unknown quantum system, and sends Bob the classical result of this measurement. Knowing this, Bob can convert the state of his EPR particle into an exact replica of the unknown state $|\phi\rangle$ which Alice destroyed.

1 2 3 4

PACS numbers: 03.65.Bz, 42.50.Dv, 89.70.+c



The discoverers of quantum teleportation meet six years later to witness application of their technique. In the first picture the teleportus has not yet undergone the final Pauli rotation.

Photo-credit: Charles Bennett, Cambridge UK 1999.

Remarks:

0. What is teleported, the body or the soul ?

Vote !!!

Remarks:

0. What is teleported, the body or the soul ?

1. Alice's operations are independent of a,b.
   The method works on a copy of the qubit, and
   no knowledge of the state is needed.

Remarks:

0. What is teleported, the body or the soul ?

1. Alice's operations are independent of a,b.
   The method works on a copy of the qubit, and
   no knowledge of the state is needed.

2. Generalizes to higher dimension (use the
   unitaries and the basis discussed at the end
   of superdense coding).

Remarks:

0. What is teleported, the body or the soul ?

1. Alice's operations are independent of a,b.
   The method works on a copy of the qubit, and
   no knowledge of the state is needed.

2. Generalizes to higher dimension (use the
   unitaries and the basis discussed at the end
   of superdense coding).

3. Preserves global state (including entanglement
   of the communicated system with anything else)
   if applied to one of two systems. (Proof: A2)

4. By 3, we can teleport a 2^n-dim system by teleporting the n qubits one by one.

Exercise: check that Alice can communicate:

$$\frac{1}{\sqrt{84}}\left(5|00\rangle + 3|10\rangle + |01\rangle + 7|11\rangle\right)$$

by teleporting the 1st qubit, and then teleporting the 2nd qubit, each using the method on p20.

4. By 3, we can teleport a 2^n-dim system by teleporting the n qubits one by one.

5. We say that teleportation uses 1 ebit and sends 2 classical bits to communicate 1 qubit.

4. By 3, we can teleport a 2^n-dim system by teleporting the n qubits one by one.

5. We say that teleportation uses 1 ebit and sends 2 classical bits to communicate 1 qubit.

6. Alice's Bell measurement learns nothing about the communicated qubit. This is necessary, else, she can learn information about the qubit without disturbing it, making non-orthogonal states more distinguishable than possible.

7. Teleportation, besides being a useful communication protocol, IS the conceptual tool for numerous important results:

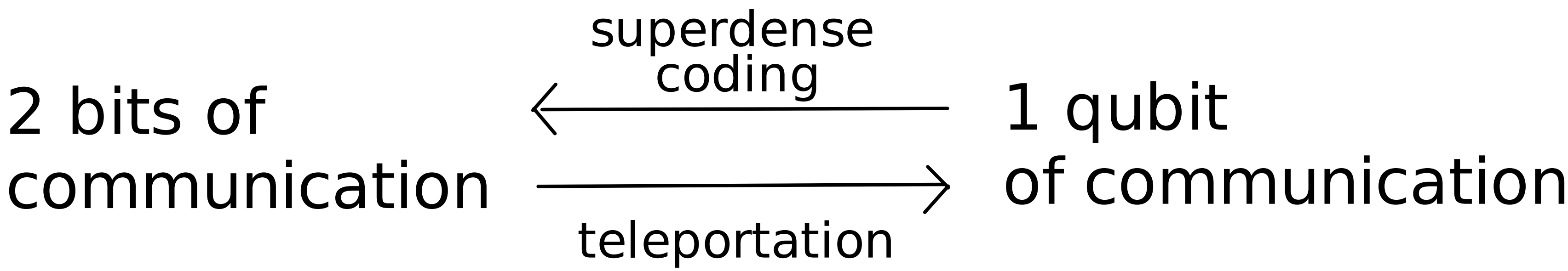
- fault tolerant quantum gates
- programmable gate arrays
- reducing quantum error correction to entanglement purification
- measurement-based quantum computation
- quantum encryption
- quantum authentication
- blind / delegated quantum computation ...

Superdense coding and teleportation:

If entanglement is free, these two communication protocols are inverses of one another:

Superdense coding and teleportation:

If entanglement is free, these two communication protocols are inverses of one another:



Superdense coding and teleportation:

If entanglement is free, these two communication protocols are inverses of one another:

2 bits of communication ← superdense coding — 1 qubit of communication

2 bits of communication — teleportation → 1 qubit of communication

Furthemore, each protocol is optimal, because of the other protocol !

in a way that preserves entanglement with the qubit

Optimality of teleportation:

Any method to communicate one qubit using entanglement must send at least 2 bits.

Optimality of teleportation:

in a way that preserves entanglement with the qubit

Any method to communicate one qubit using entanglement must send at least 2 bits.

Proof:

Suppose, by contradiction, there is a method T to communicate a qubit while consuming some entangled state $|\mu\rangle$ and sending c < 2 classical bits.

Idea: if X is too good to be true, compose it with something else Y that's is known to be true, and get something new Z so good that it's an immediate contradiction.

Optimality of teleportation:

in a way that preserves entanglement with the qubit

Any method to communicate one qubit using entanglement must send at least 2 bits.

Proof:

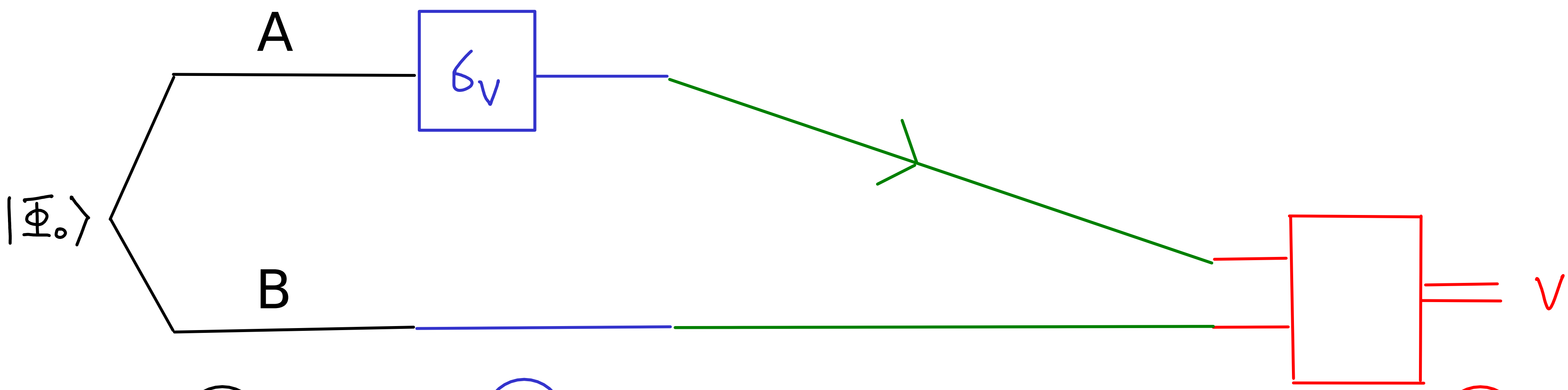
Suppose, by contradiction, there is a method T to communicate a qubit while consuming some entangled state $|\mu\rangle$ and sending c < 2 classical bits.

Idea: if X is too good to be true, compose it with something else Y that's is known to be true, and get something new Z so good that it's an immediate contradiction.

X: method T sending fewer than 2 classical bits
Y: known standard superdense coding
Composition: use method T to comm the qubit in Y
Z: sending too much classical data with entanglement

Superdense coding (proven to work):

(3) Alice sends system C=A to Bob (2-dim).



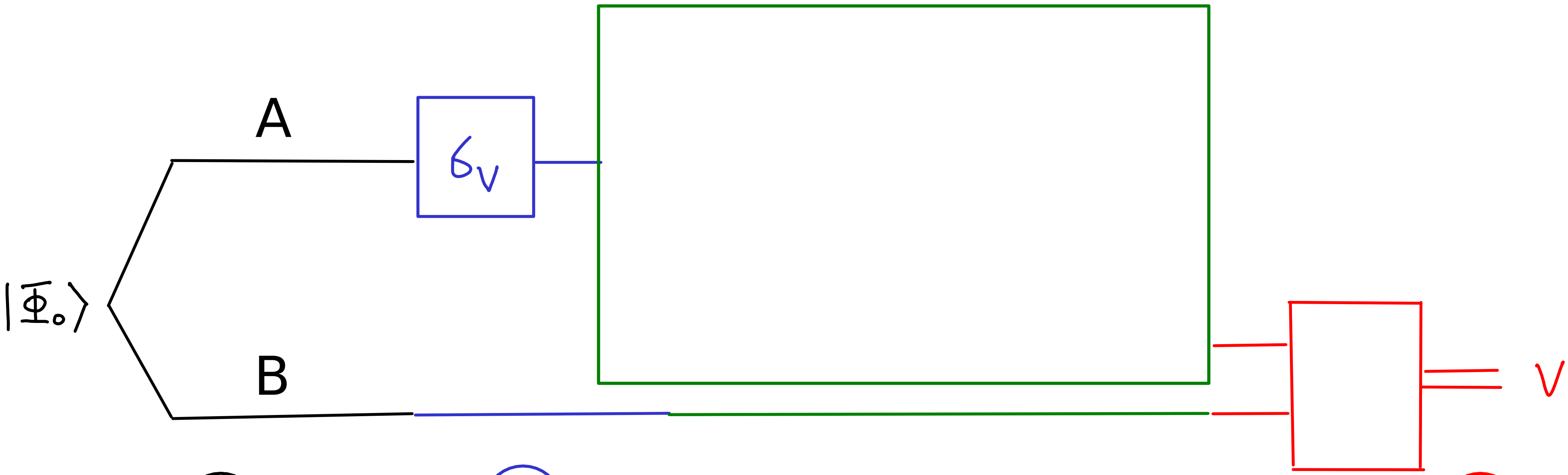
(1) ebit shared by Alice (A) and Bob (B)

(2) To comm "v" Alice applies Pauli-v, for v in {0,x,y,z}.

(4) Bob measures along the Bell basis to get v.

Superdense coding (still works if method T exists):

③ Alice ~~sends~~ comm system C=A to Bob (2-dim)
USING METHOD T.



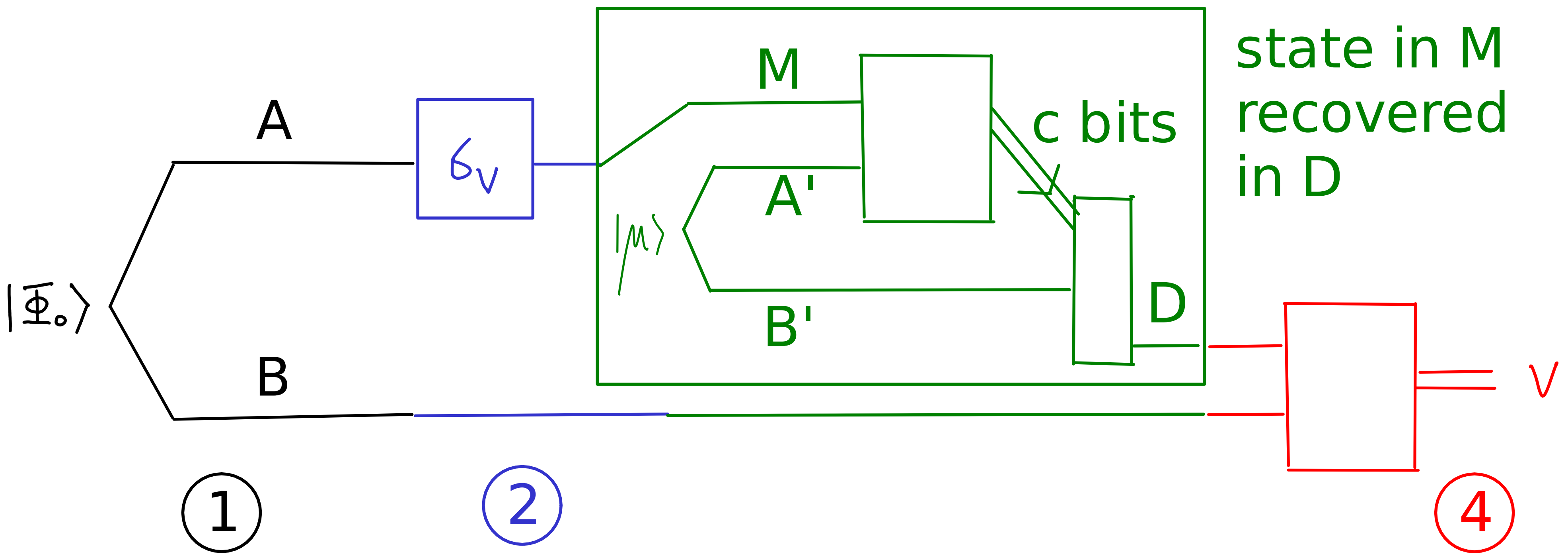
① ebit shared by Alice (A) and Bob (B)

② To comm "v" Alice applies Pauli-v, for v in {0,x,y,z}.

④ Bob measures along the Bell basis to get v.

Superdense coding (still works if method T exists):

③ Alice ~~sends~~ comm system C=A to Bob (2-dim)
USING METHOD T.



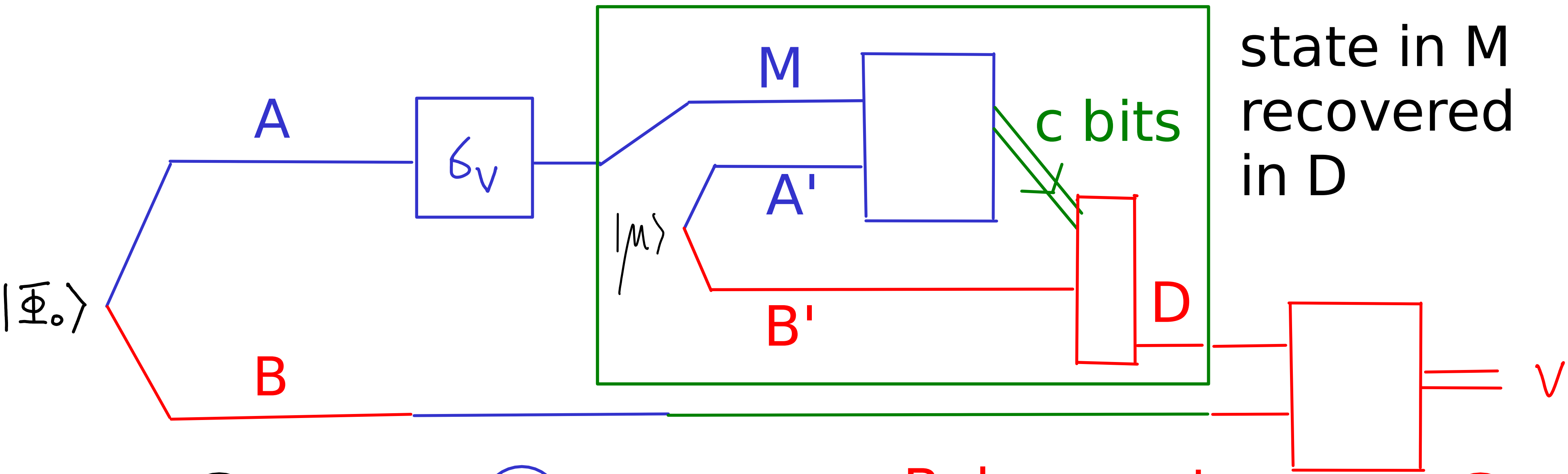
ebit shared by Alice (A) and Bob (B)

To comm "v" Alice applies Pauli-v, for v in {0,x,y,z}.

Bob measures along the Bell basis to get v.

Z: new method to send 2 classical bits v using c bits & entanglement

③ Alice sends c bits to Bob



state in M recovered in D

① ebit shared by Alice (A) and Bob (B)

② To comm "v" Alice applies Pauli-v, for v in {0,x,y,z}.

Alice also operates on M and A'.

Bob operates on D, then

④ Bob measures along the Bell basis to get v.

Optimality of teleportation:

in a way that preserves entanglement with the qubit

Any method to communicate one qubit using entanglement must send at least 2 bits.

Proof:
Suppose, by contradiction, there is a method T to communicate a qubit while consuming some entangled state $|\mu\rangle$ and sending c < 2 classical bits.

Then, take superdense coding scheme, and send the qubit in SD coding by method T.

New scheme now communicates 2 bits using $|\mu\rangle, |\Phi_0\rangle$ and by sending c < 2 bits.

This contradicting the principle of no discounted lunch+. So, method T cannot exist.

Optimality of superdense coding:

Any method to communicate 2 bits using entanglement must send at least 1 qubit.

Proof: A2

Discuss what is expected of the answer.

NB. Both optimality proofs assume asymptotically large number of uses, and consider the average rate.

From the original teleportation paper:

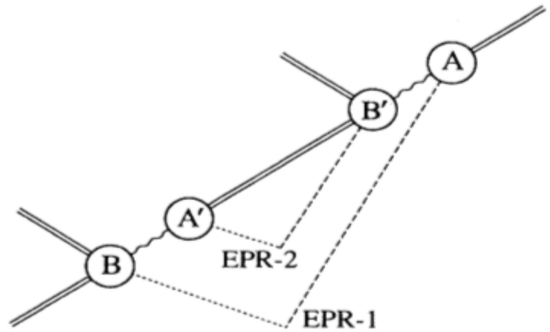


figure drawn as a postscript file by the late Asher Peres

FIG. 2. Spacetime diagram of a more complex 4-way coding scheme in which the modulated EPR particle (wavy line) is teleported rather than being transmitted directly. This diagram can be used to prove that a classical channel of two bits of capacity is necessary for teleportation. To do so, assume on the contrary that the teleportation from A' to B' uses an internal classical channel of capacity $C < 2$ bits, but is still able to transmit the wavy particle's state accurately from A' to B', and therefore still transmit the external two-bit message accurately from B to A. The assumed lower capacity $C < 2$ of the internal channel means that if B' were to guess the internal classical message superluminally instead of waiting for it to arrive, his probability 2^{-C} of guessing correctly would exceed 1/4, resulting in a probability greater than 1/4 for successful superluminal transmission of the external two-bit message from B to A. This in turn entails the existence of two distinct external two-bit messages, r and s, such that $P(r|s)$, the probability of superluminally receiving r if s was sent, is less than 1/4, while $P(r|r)$, the probability of superluminally receiving r if r was sent, is greater than 1/4. By redundant coding, even this statistical difference between r and s could be used to send reliable superluminal messages; therefore reliable teleportation of a two-state particle cannot be achieved with a classical channel of less than two bits of capacity. By the same argument, reliable teleportation of an N-state particle requires a classical channel of $2\log_2(N)$ bits capacity.

superdense coding

no discounted lunch principle

4. Immediate information processing consequences of QM

i.e., more examples of QM :)

✓ (a) No-cloning theorem (NC 1.3.5, box 12.1)

✓ (b) Non-distinguishability of non-orthogonal states (NC p56-57)

✓ (c) Communication of data
- protocols, bounds, and non-signalling principle
- encoding and extraction of classical data in QM

✓ (d) Superdense coding and teleportation (NC 2.3, 1.3.7, KLM 5.1-5.2, N 6.4-6.5)

→ (e) Bell's inequality and nonlocal games (NC 2.6, M 6.6)

We saw that entanglement does not:

(1) allow signalling

(2) increase the # bits communicated by a noiseless classical channel.

We saw that entanglement does not:

(1) allow signalling

(2) increase the # bits communicated by a noiseless classical channel.

But it offers quantum advantages when it is used with a channel:

(3) it converts a noiseless bit channel into a quantum channel (teleportation)

(4) it doubles the classical bit rate of the noiseless quantum channel (superdense coding)

We saw that entanglement does not:

(1) allow signalling

(2) increase the # bits communicated by a noiseless classical channel.

But it offers quantum advantages when it is used with a channel:

(3) it converts a noiseless bit channel into a quantum channel (teleportation)

(4) it doubles the classical bit rate of the noiseless quantum channel (superdense coding)

We will see that entanglement can produce correlations that are impossible to obtain classically, why this doesn't contradict item (1), and why this is interesting.

Bell's inequality

view from physics

Nonlocal games

view from computer science

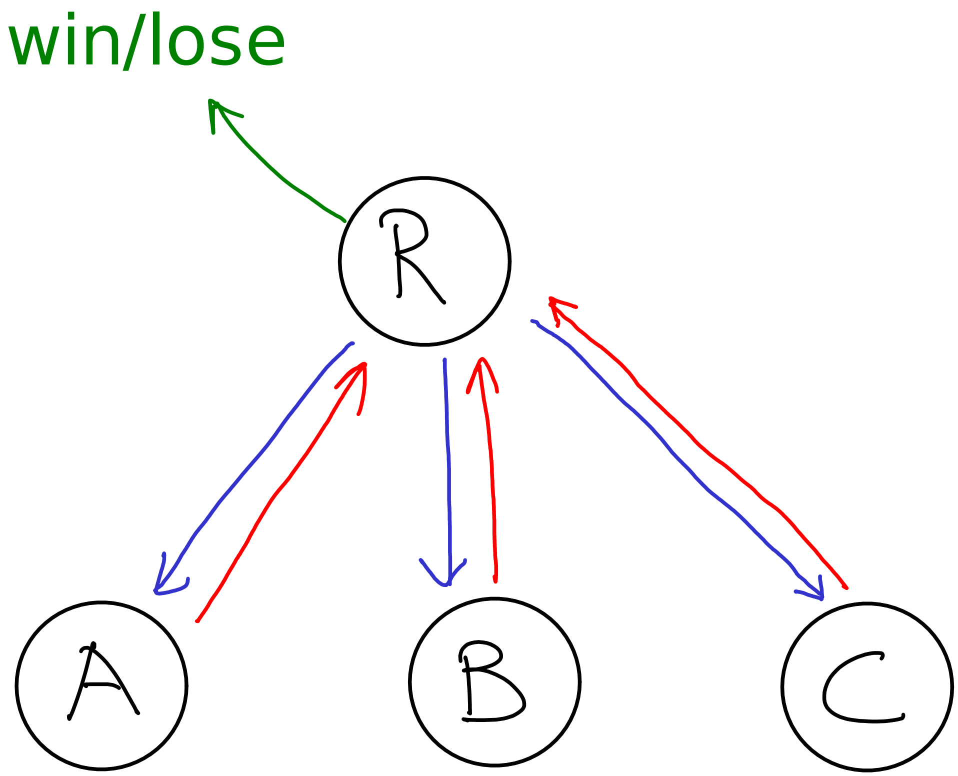
clearer motivations and less confusing

Scenario:

A referee "runs" a game G with a list of k players (Alice, Bob, Charlie, ...).

All communication in the game is between the referee and each individual player. The players do NOT communicate to one another during the game.

Example: the GHZ game



k = 3 players A, B, C

Scenario:

A referee "runs" a game G with a list of k players (Alice, Bob, Charlie, ...).

All communication in the game is between the referee and each individual player. The players do NOT communicate to one another during the game.

BEFORE the game, the players can agree on a strategy and share correlations. The players win or lose collectively as a team.

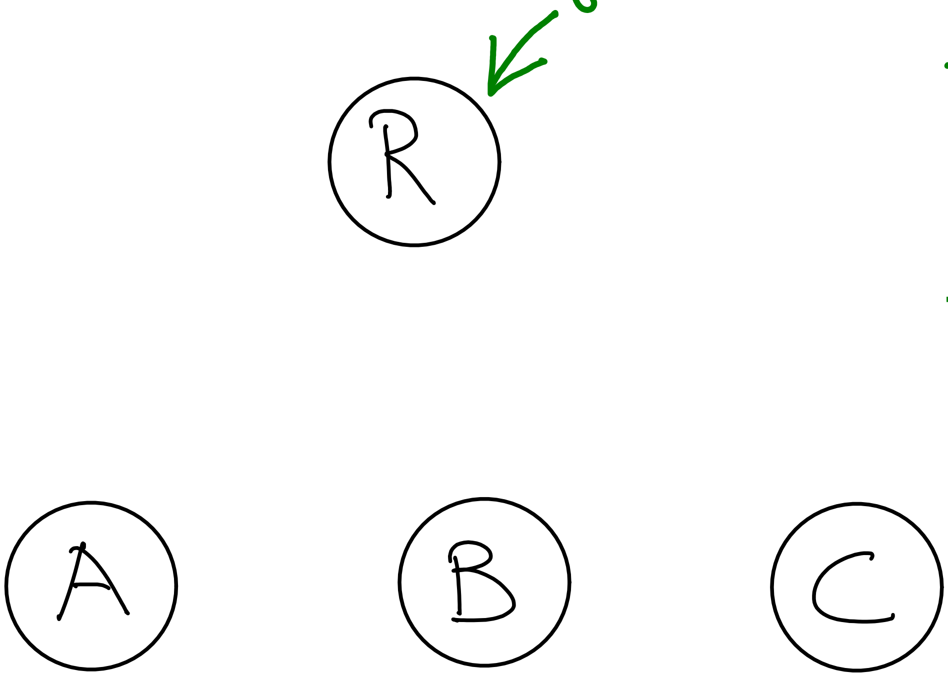
During the game:

(1) The referee draws a "query" q from a list L, according to a distribution p. Each query is a k-tuple (ordered) of questions, one for each player.

Example: the GHZ game

$q = (r, s, t) \in_R \{000, 011, 101, 110\} = L$

p: uniform over L in this game



each query has 3 bits,
j-th bit is the question
to the j-th party

k = 3 players A, B, C

During the game:

(1) The referee draws a "query" q from a list L, according to a distribution p. Each query is a k-tuple (ordered) of questions, one for each player.

(2) The referee sends each question to the corresponding player.

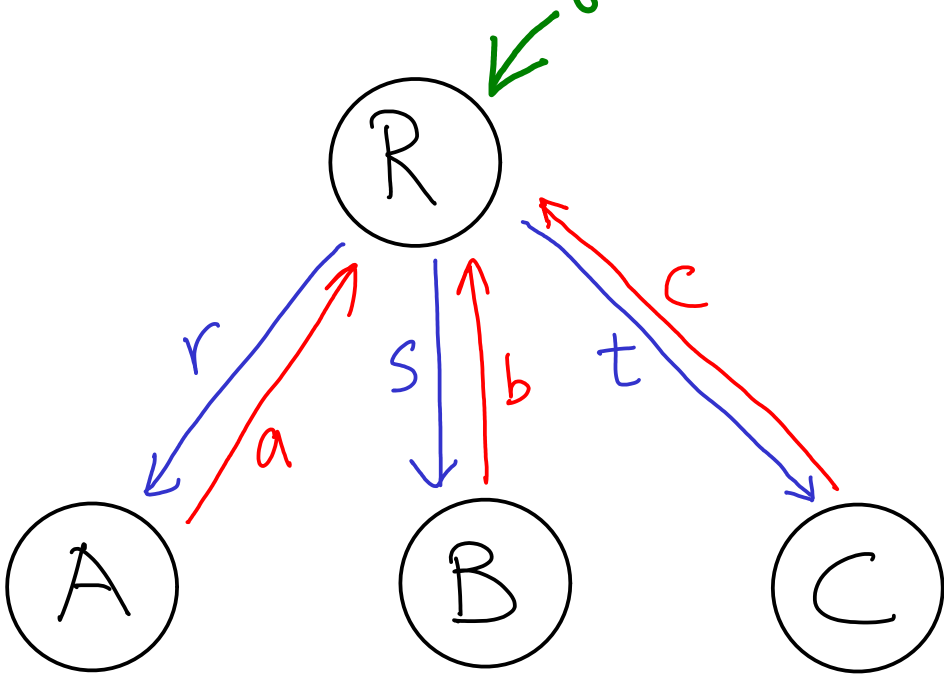
(3) Each player returns an answer to the referee.

Example: the GHZ game

$q = (r, s, t) \in_R \{000, 011, 101, 110\} = L$

p: uniform over L in this game

$a, b, c \in \{0, 1\}$



k = 3 players A, B, C

During the game:

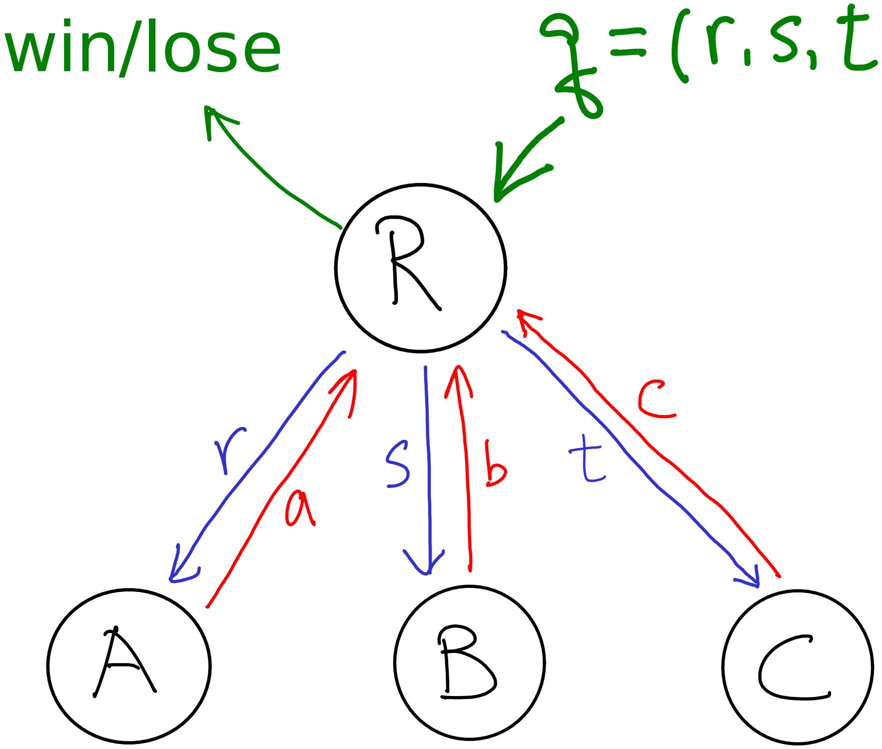
(1) The referee draws a "query" q from a list L, according to a distribution p. Each query is a k-tuple (ordered) of questions, one for each player.

(2) The referee sends each question to the corresponding player.

(3) Each player returns an answer to the referee.

(4) Based on the query and the joint answers, the referee decides whether the players win or lose.

Example: the GHZ game



$q = (r, s, t) \in_R \{000, 011, 101, 110\} = L$

p: uniform over L in this game

$a, b, c \in \{0, 1\}$

Winning condition:

$a \oplus b \oplus c \bmod 2 = r \vee s \vee t$

i.e., parity of (a,b,c) is:

$\begin{cases} \text{even if } rst = 000, \\ \text{odd} \quad \text{if } rst = 011, 101, 110 \end{cases}$

During the game:

(1) The referee draws a "query" q from a list L, according to a distribution p. Each query is a k-tuple (ordered) of questions, one for each player.

(2) The referee sends each question to the corresponding player.

(3) Each player returns an answer to the referee.

(4) Based on the query and the joint answers, the referee decides whether the players win or lose.

Scenario:

The game G is defined by
k: the number of players,
L: the list of queries,
p: the distribution of queries,
the range for the answers,
the "winning conditions" in step (4).

} known to referee & all parties

The referee plays honestly, and the players want to maximize their probability of winning.

Scenario:

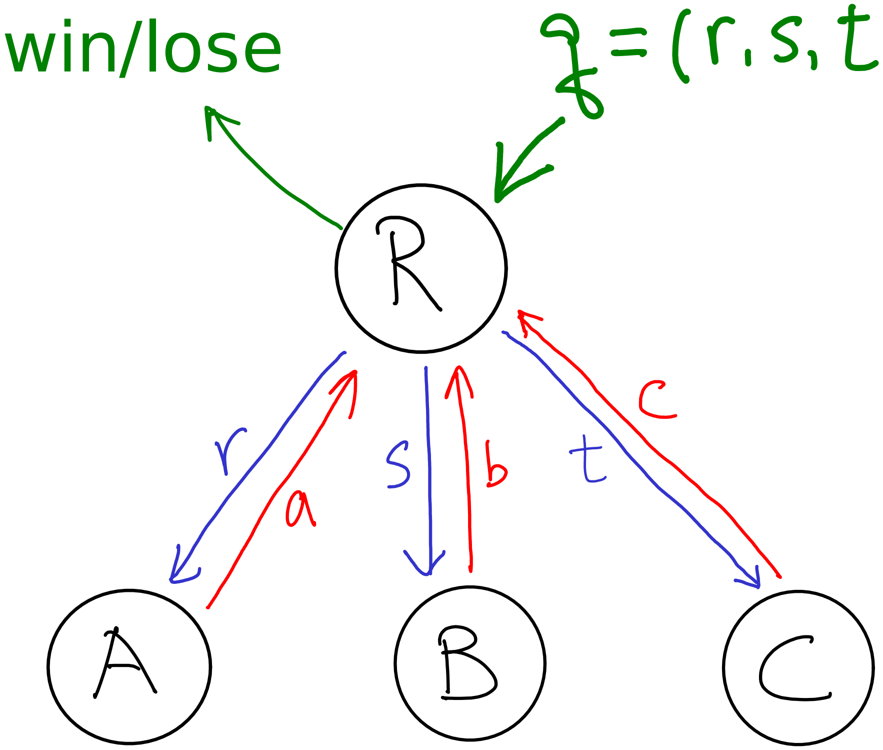
The game G is defined by
k: the number of players,
L: the list of queries,
p: the distribution of queries,
the range for the answers,
the "winning conditions" in step (4).

} known to referee & all parties

The referee plays honestly, and the players want to maximize their probability of winning.

Crux: each player only sees his/her question, so q is only partially known to each player. This limits their coordination to win.

Example: the GHZ game



$q = (r, s, t) \in_R \{000, 011, 101, 110\} = L$

p: uniform over L in this game

$a, b, c \in \{0, 1\}$

Winning condition:

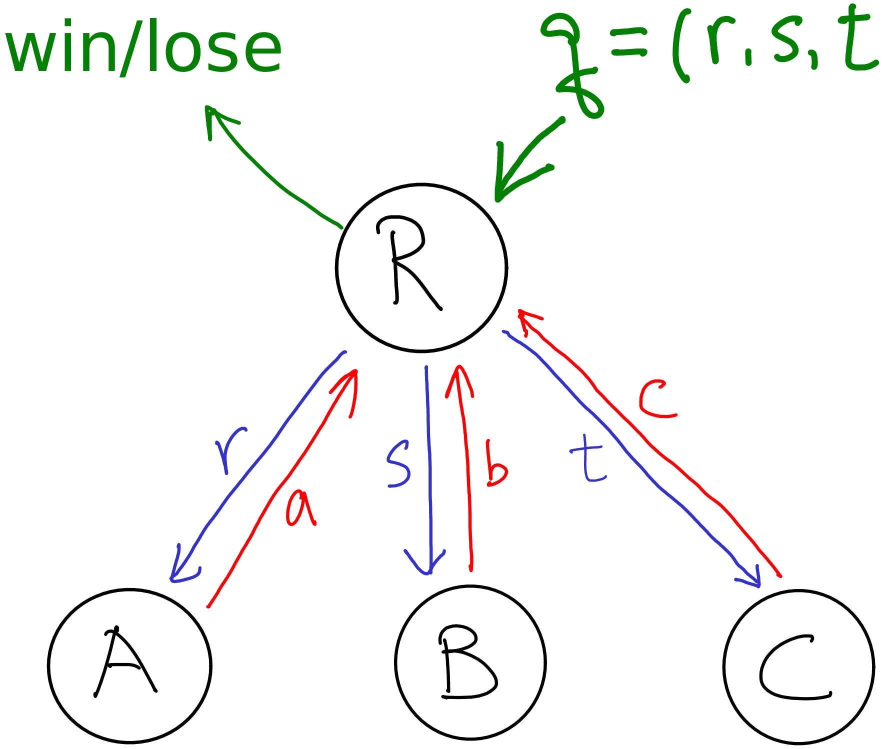
$a \oplus b \oplus c \bmod 2 = r \vee s \vee t$

i.e., parity of (a,b,c) is:

$\begin{cases} \text{even if rst = 000,} \\ \text{odd if rst = 011, 101, 110} \end{cases}$

Here each player learns 1 bit about q but not q itself.
e.g., If Bob receives 0, q=000 or 101.

Example: the GHZ game



$q = (r, s, t) \in_R \{000, 011, 101, 110\} = L$

p: uniform over L in this game

$a, b, c \in \{0, 1\}$

Winning condition:

$a \oplus b \oplus c \bmod 2 = r \vee s \vee t$

i.e., parity of (a,b,c) is:

$$\begin{cases} \text{even if } rst = 000, \\ \text{odd} \quad \text{if } rst = 011, 101, 110 \end{cases}$$

Claim:

Best classical strategy wins with probability 3/4.
Best quantum strategy wins with certainty !

type of correlations and operations

Deterministic classical strategy for the GHZ game

Each player has a deterministic answer for each possible question. e.g.,

Alice's answer is $a=a0$ if $r=0$, $a=a1$ if $r=1$.

Remember Alice only knows r but not know s or t.

Deterministic classical strategy for the GHZ game

Each player has a deterministic answer for each possible question.

Alice's answer is $a=a0$ if $r=0$, $a=a1$ if $r=1$.
Bob's answer is $b=b0$ if $s=0$, $b=b1$ if $s=1$.
Charlie's answer is $c=c0$ if $t=0$, $c=c1$ if $t=1$.

So, the 6 bits a0,...,c1 species any deterministic classical strategy.

How good are the deterministic classical strategies?

(1) The parties must lose at least 1 query.

Proof (by contradiction): Suppose there is a strategy, specified by a0, a1, ..., c1 that enables the parties to always win. Then,

How good are the deterministic classical strategies?

(1) The parties must lose at least 1 query.

Proof (by contradiction): Suppose there is a strategy, specified by a0, a1, ..., c1 that enables the parties to always win. Then,

$$a_0 \oplus b_0 \oplus c_0 = 0$$ (when rst=000, the answer bits need to have even parity to win)

$$a_0 \oplus b_1 \oplus c_1 = 1$$ (when rst=011, the answer bits need to have odd parity to win)

$$a_1 \oplus b_1 \oplus c_0 = 1$$ ⋮

$$a_1 \oplus b_0 \oplus c_1 = 1$$

How good are the deterministic classical strategies?

(1) The parties must lose at least 1 query.

Proof (by contradiction): Suppose there is a strategy, specified by a0, a1, ..., c1 that enables the parties to always win. Then,

$$a_0 \oplus b_0 \oplus c_0 = 0$$ (when rst=000, the answer bits need to have even parity to win)

$$a_0 \oplus b_1 \oplus c_1 = 1$$ (when rst=011, the answer bits need to have odd parity to win)

$$a_1 \oplus b_1 \oplus c_0 = 1$$ ⋮

$$a_1 \oplus b_0 \oplus c_1 = 1$$

Then, if we sum the 4 equations above,
LHS = 0 mod 2, RHS = 1 mod 2 (contradiction).

How good are the deterministic classical strategies?

(2) The winning probability is at most 3/4, since the parties lose in at least one query, each is drawn with probability 1/4.

How good are the deterministic classical strategies?

(2) The winning probability is at most 3/4, since the parties lose in at least one query, each is drawn with probability 1/4.

(3) It is easy to win with probability 3/4.
e.g., take a0=b0=c0=1, a1=b1=c1=0.
Then, the parties lose in the first query 000
(their joint answer 111 has odd parity),
but they always win the rest
(e.g., for 110, the answers 001 has odd parity).

most general

How good are the ~~deterministic~~ classical strategies?

Most generally, the parties can share randomness. For each random value, they follow a strategy, which in turns uses local randomness.

The overall winning probability is the winning prob averaged over all shared and local random variables.

most general

How good are the ~~deterministic~~ classical strategies?

Most generally, the parties can share randomness.
For each random value, they follow a strategy, which in turns uses local randomness.

The overall winning probability is the winning prob averaged over all shared and local random variables.

By convexity, this average is no better than the best case (over random variables) winning probability, which is given by some deterministic strategy.

This conclude the first claim, that the best classical strategy wins with probabilty 3/4.

Quantum strategy for general nonlocal games

The players can share an entangled state before the game starts.

For each player, for each question, a measurement that depends on the question is applied on the entangled state. Each answer depends on both the question and the measurement outcome.

Quantum strategy for the GHZ game

The players share a (surprise!) GHZ state:

$$|\gamma\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$$

↑ Greenberger-Horne-Zeilinger

Quantum strategy for the GHZ game

The players share a (surprise!) GHZ state:

$$|\gamma\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

↑ Greenberger-Horne-Zeilinger

For each player:

If the question is 0, measure eigenspace of σ_x

1 σ_y.

If measurement outcome is +1, answer = 0

-1 1.

Why do they always win?

In A1 Q4, you show that:

For a state $|\psi\rangle$,

S1, S2 hermitian operators with eigenvalues +/- 1,

If $S_1 \otimes S_2 |\psi\rangle = |\psi\rangle$

then, measuring S1, S2 locally, separately, gives two outcomes u and v such that uv is always +1.

i.e., only (u,v) = (+1,+1) or (-1,-1) occurs.

In A1 Q4, you show that:

For a state $|\Psi\rangle$,

S1, S2 hermitian operators with eigenvalues +/- 1,

If $S_1 \otimes S_2 |\Psi\rangle = |\Psi\rangle$

then, measuring S1, S2 locally, separately, gives two outcomes u and v such that uv is always +1.

i.e., only (u,v) = (+1,+1) or (-1,-1) occurs.

If $S_1 \otimes S_2 |\Psi\rangle = -|\Psi\rangle$, uv is always -1.

i.e., only (u,v) = (+1,-1) or (-1,+1) occurs.

In A1 Q4, you show that:

For a state $|\psi\rangle$,

S1, S2 hermitian operators with eigenvalues +/- 1,

If $S_1 \otimes S_2 |\psi\rangle = |\psi\rangle$

then, measuring S1, S2 locally, separately, gives two outcomes u and v such that uv is always +1.

i.e., only (u,v) = (+1,+1) or (-1,-1) occurs.

If $S_1 \otimes S_2 |\psi\rangle = -|\psi\rangle$, uv is always -1.

i.e., only (u,v) = (+1,-1) or (-1,+1) occurs.

This extends to any number of systems by induction, in particular, to k=3 qubits.

Quantum strategy for the GHZ game

The players share $|\gamma\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

which is a +1 eigenstate of $\sigma_x \otimes \sigma_x \otimes \sigma_x$,

and a -1 eigenstate of $\sigma_y \otimes \sigma_y \otimes \sigma_x$,

$\sigma_y \otimes \sigma_x \otimes \sigma_y$,

$\sigma_x \otimes \sigma_y \otimes \sigma_y$. (Exercise)

Recall: Each of σ_x and σ_y has eigenvalues +/- 1.

Quantum strategy for the GHZ game

The players share $|\gamma\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

which is a +1 eigenstate of $\sigma_x \otimes \sigma_x \otimes \sigma_x$,

and a -1 eigenstate of $\sigma_y \otimes \sigma_y \otimes \sigma_x$,

$\sigma_y \otimes \sigma_x \otimes \sigma_y$,

$\sigma_x \otimes \sigma_y \otimes \sigma_y$. (Exercise)

If the query is 000, each of ABC measures σ_x and the product of the 3 outcomes is always +1 (A1Q4). Converting +1 to 0, and -1 to 1, a+b+c = 0 mod 2.

So they win.

Quantum strategy for the GHZ game

The players share $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

which is a +1 eigenstate of $\sigma_x \otimes \sigma_x \otimes \sigma_x$,

and a -1 eigenstate of $\sigma_y \otimes \sigma_y \otimes \sigma_x$,

$\sigma_y \otimes \sigma_x \otimes \sigma_y$,

$\sigma_x \otimes \sigma_y \otimes \sigma_y$. (Exercise)

If the query is 000, each of ABC measures σ_x and the product of the 3 outcomes is always +1 (A1Q4). Converting +1 to 0, and -1 to 1, a+b+c = 0 mod 2.

If the query is 110, 101, or 011, measuring σ_x on one qubit, and σ_y on the others, outcomes have product -1, so a+b+c = 1 mod 2. So, they also win.

So, the quantum strategy has winning prob 1 !

Summary: in nonlocal games, remote parties can overcome their lack of information on the query using quantum correlations that are extracted by quantum measurements.

In the GHZ game, a quantum strategy has winning probability 1, while the best classical strategy has winning probability 3/4.

Summary: in nonlocal games, remote parties can overcome their lack of information on the query using quantum correlations that are extracted by quantum measurements.

In the GHZ game, a quantum strategy has winning probability 1, while the best classical strategy has winning probability 3/4.

Can such quantum correlation enable signalling between the parties?

Summary: in nonlocal games, remote parties can overcome their lack of information on the query using quantum correlations that are extracted by quantum measurements.

In the GHZ game, a quantum strategy has winning probability 1, while the best classical strategy has winning probability 3/4.

Can such quantum correlation enable signalling between the parties?

No. No party can affect the outcome distribution of any other. You prove that in A1Q3 (for 2 parties)!
The non-classical correlation in the JOINT answer is only observed by the referee (he talks to all 3 parties).
Marginal distribution for each party does not depend on what the other two parties are doing.

Remark: the prob of winning is not a measurement outcome ... and cannot be observed directly, not even to the referee. To verify the correlation, independent copies of the game should be played, and the winning prob estimated. A method to enforce independence is needed.

Remark: the prob of winning is not a measurement outcome ... and cannot be observed directly, not even to the referee. To verify the correlation, independent copies of the game should be played, and the winning prob estimated. A method to enforce independence is needed.

But these can be done, and in fact, with advanced techniques, the referee can verify that the parties share the optimal state and perform the optimal measurements. That's allows very secure quantum key distribution wherein the referee does not even need to do anything quantum!

Similarly for delegated computation.

Connecting nonlocal games to Bell inequalities:

Nonlocal game	Bell inequality
Questions	Measurement settings
Answers	Measurement outcomes
No communication	Spacelike separated

Connecting nonlocal games to Bell inequalities:

Nonlocal game	Bell inequality
Questions	Measurement settings
Answers	Measurement outcomes
No communication	Spacelike separated
Winning prob	Expectation of a function of the observables e.g. $\sigma_x \otimes \sigma_x \otimes \sigma_x - \sigma_y \otimes \sigma_y \otimes \sigma_x - \sigma_y \otimes \sigma_x \otimes \sigma_y - \sigma_x \otimes \sigma_y \otimes \sigma_y$ Bell's inequality: upper bound the expectation, given shared randomness (local hidden variable model).

Connecting nonlocal games to Bell inequalities:

Nonlocal game	Bell inequality
Questions	Measurement settings
Answers	Measurement outcomes
No communication	Spacelike separated
Winning prob	Expectation of a function of the observables e.g. $\sigma_x \otimes \sigma_x \otimes \sigma_x - \sigma_y \otimes \sigma_y \otimes \sigma_x - \sigma_y \otimes \sigma_x \otimes \sigma_y - \sigma_x \otimes \sigma_y \otimes \sigma_y$ Bell's inequality: upper bound the expectation, given shared randomness (local hidden variable model).
Entanglement strictly increases winning probability	QM violates the Bell's inequality.

In physics, the main interest in Bell inequalities come from the fact that it refutes local hidden variables.

In recent years, "loopholes-free demonstrations" have been reported.

Note this does not verify quantum mechanics, but rules out the obvious competing physical theory.

Further opportunities to study quantum subjects:

Graduate courses at IQC :

Quantum information -- DL (F23, F25?)

Quantum communication -- DL (F20)

(W19)

Nonlocal games and entanglement -- Professor Cleve

Quantum entanglement -- Professor G Smith (W25)

Quantum algorithms -- Professor Gosset (S23, 25?)

Quantum error correction & fault tolerance --
DL, Yoshida, Vasmer (W22, 24, ?)